Docket No.: 2565-0297PUS1
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of: Takehiro OHKOSHI et al.	**Before the Board of Appeals**
Application No.: 10/584,194	Confirmation No.: 1262
Filed: May 25, 2007	Art Unit: 2431
For: AUTHENTICATED DEVICE, AUTHENTICATING DEVICE AND AUTHENTICATING METHOD	Examiner: Kaveh ABRISHAMKAR

REPLY BRIEF

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Appellants submit herewith a Reply Brief. This Brief on Appeal responds to the Examiner's Answer dated January 26, 2010.

For clarity, the issues presented in the Appeal Brief filed October 5, 2009, will be repeated, and the Reply to the Examiner's Answer will correspond structurally to the arguments section in the Appeal Brief.

I. ISSUE ON APPEAL

The issue to be resolved in this application is:

Whether claims 1-10 are properly rejected under 35 USC 102(e) as being anticipated by Edgett et al. (U.S. Patent Publication No. US 2004/0034771; hereinafter "Edgett").

II. NEW POINTS OF ARGUMENT RAISED BY THE EXAMINER'S ANSWER

Appellants are providing this Reply Brief to respond to new points of argument raised in the Examiner's Answer. Appellants do not disagree with paragraphs (1)-(8) of the Examiner's Answer. Appellants disagree with new points of argument with regard to independent claims 1, 4 and 7-10 in paragraph (9) and (10) introduced by the Examiner. Appellants' response to these assertions is provided below.

III. REPLY

A. The Rejection Fails to Establish *Prima Facie* Anticipation of Independent Claim 1

Independent claims 1 recites, *inter alia*,

> a transmitting unit to transmit the at least one algorithm identifier and the at least one encryption key identifier stored by the memory unit to an authenticating device;
>
> a receiving unit to receive a prescribed algorithm identifier and a prescribed encryption key identifier, which are selected from among the at least one algorithm identifier and the at least one encryption key identifier transmitted by the transmitting unit.

Appellants respectfully submit that the Examiner's reasoning provided in support of the rejection of independent claim 1 under 35 U.S.C. § 102(e) as being anticipated by Edgett fails to establish *prima facie* anticipation. The deficiencies of the rejection are at least in that Edgett fails to disclose the above-noted features of independent claim 1.

In response to the Appellants' arguments regarding claim 1, the Examiner responds with new arguments on the interpretation of the teachings of Edgett. Specifically, the Examiner asserts in the Examiner's Answer on pages 15 and 16 as follows:

> ...Edgett teaches receiving a prescribed algorithm identifier selected from the at lest one algorithm identifier and the at least one encryption key identifier...[t]he Update Server, which together with the decryption server comprises the authenticating device (both functionalities can be housed on the same device/server) then sends which algorithm is to be employed in further communications and transmits the updated encryption key index and algorithm identifier back to the authenticated network user (authenticated device) (paragraph 0059) when the algorithm is updated (paragraph (0059).
>
> ...Edgett teaches receiving a prescribed encryption key identifier which is selected from among the at least one algorithm identifier and the at least on encryption key identifier transmitted by the transmitting unit...[t]he Update Server, which together with the decryption server comprises the authenticating device (both functionalities can be housed on the same device/server) then sends which algorithm is to be employed in further communications and transmits the key with its associated key index to the network user when authenticated (authenticated network user) (paragraph 0055).

In view of the above arguments, the Examiner appears to disregard or misread the claimed features as well as to mischaracterize Edgett in an effort to satisfy the claimed features. Claim 1 is directed to an authenticated device including, *inter alia,* a receiving unit to receive

from a authenticating device a prescribed algorithm identifier and a prescribed encryption key identifier, **selected from among the at least one algorithm identifier and the at least one encryption key identifier transmitted by the transmitting unit**. As such, the prescribed algorithm identifier and the prescribed encryption key identifier received by the claimed authenticated device are among the at least one algorithm identifier and the at least one encryption key identifier transmitted by the claimed authenticated device.

In contrast, Edgett discloses that, during an authentication process, a user transmits an old algorithm identifier and an old encryption key index to the decryption/Update servers. Edgett further discloses that, during an updating process, the decryption/Update servers transmit a new (updated) algorithm identifier and a new (updated) encryption key index to the user. As such, the new (updated) algorithm identifier and new (updated) encryption key index **received by the user** cannot be, and are NOT selected among the old algorithm identifier and the old encryption **transmitted by the user.**

In fact, as pointed out by the Examiner, Edgett discloses that the Update Server sends back to the network user the updated algorithm to be employed in further communications and the **updated** encryption key index and the **updated** algorithm identifier when the algorithm is updated. See pages 15 and 16 of the Examiner's Answer. As such, by definition, the **updated** encryption key index and the **updated** algorithm identifier to be employed in further communications cannot also be the old encryption key index and the old updated algorithm identifier that were previously transmitted by the user.

Thus, Edgett fails to disclose or suggest at least "a receiving unit to receive from a authenticating device a prescribed algorithm identifier and a prescribed encryption key identifier,

selected from among the at least one algorithm identifier and the at least one encryption key identifier transmitted by the transmitting unit" as claimed.

As such, Appellants maintain that the Examiner has failed to establish *prima facie* anticipation in the rejection of claim 1.

B. The Rejection Fails to Establish *Prima Facie* Anticipation of Independent Claim 4

Independent claims 4 recites, *inter alia*,

> a selecting unit to select a prescribed algorithm identifier and a prescribed encryption key identifier to be stored by the memory unit from among the at least one algorithm identifier and the at least one encryption key identifier received by the receiving unit, when the at least one algorithm identifier and the at least one encryption key identifier stored by the memory unit exist among the at least one algorithm identifier and the at least one encryption key identifier received by the receiving unit;
>
> a transmitting unit to transmit the prescribed algorithm identifier and the prescribed encryption key identifier selected by the selecting unit to the authenticated device.

Appellants respectfully submit that the Examiner's reasoning provided in support of the rejection of independent claim 4 under 35 U.S.C. § 102(e) as being anticipated by Edgett fails to establish *prima facie* anticipation. The deficiencies of the rejection are at least in that Edgett fails to disclose the above-noted features of independent claim 4.

In response to the Appellants' arguments regarding claim 4, the Examiner responds with new arguments on the interpretation of the teachings of Edgett. Specifically, the Examiner asserts in the Examiner's Answer on pages 16 and 17 as follows:

> ... Edgett teaches transmitting the prescribed algorithm identifier to an authenticated device. The Update Server, which together with the decryption server comprises the authenticating device (both functionalities can be housed on the same device/server) sends which algorithm is to be employed in further communications and transmits the updated encryption key index and algorithm identifier back to the authenticated network user (authenticated device) (paragraph 0059) when the algorithm is updated (paragraph (0059).
>
> ...Edgett teaches transmitting the prescribed key identifier to an authenticated device. The Update Server, which together with the decryption server comprises the authenticating device (both functionalities can be housed on the same device/server) then sends which algorithm is to be employed in further communications and transmits the key with its associated key index to the network user when authenticated (authenticated network user) (paragraph 0055).

The Examiner again appears to disregard or misread the claimed features as well as to mischaracterize Edgett in an effort to satisfy the claimed features. Claim 4 is directed to an authenticating device including, *inter alia*,

> a selecting unit **to select a prescribed algorithm identifier and a prescribed encryption key identifier to be stored by the memory unit from among the at least one algorithm identifier and the at least one encryption key identifier received by the receiving unit**, when the at least one algorithm identifier and the at least one encryption key identifier stored by the memory unit exist among the at least one algorithm identifier and the at least one encryption key identifier received by the receiving unit;
>
> a transmitting unit to transmit the prescribed algorithm identifier and the prescribed encryption key identifier **selected by the selecting unit** to the authenticated device.

Appellants do not disagree with the Examiner that Edgett disclose that the Update Server transmits updated algorithm to be employed in further communications and transmits the updated

encryption key index and the updated algorithm identifier to the user during an updating process. However, the **updated** encryption key index and **updated** algorithm identifier transmitted by the Update Server are NOT the prescribed algorithm identifier and the prescribed encryption key identifier **selected from among the at least one algorithm identifier and the at least one encryption key identifier received by the receiving unit by the selecting unit** as claimed.

In Edgett, while the Update Sever receives the old key identifier associated with the old algorithm and the old encryption key from the user during an authentication process, the **updated** encryption key index and **updated** algorithm identifier cannot be and are NOT **selected** from among the old key identifier associated with the old algorithm and the old encryption key received by Update Server. Again, by definition, an **updated** encryption key index and an **updated** algorithm identifier to be employed in further communications cannot also be the old encryption key index and the old updated algorithm identifier received by the Update Server.

Thus, Edgett fails to disclose or suggest "a selecting unit to select a prescribed algorithm identifier and a prescribed encryption key identifier to be stored by the memory unit from among the at least one algorithm identifier and the at least one encryption key identifier received by the receiving unit" and "a transmitting unit to transmit the prescribed algorithm identifier and the prescribed encryption key identifier selected by the selecting unit to the authenticated device" as claimed.

As such, Appellants maintain that the Examiner has failed to establish *prima facie* anticipation in the rejection of claim 4.

C. The Rejection Fails to Establish *Prima Facie* Anticipation of Independent Claim 7

Independent claims 7 recites, *inter alia*,

> a first transmitting step to transmit, from an authenticated device storing a plurality of algorithm identifiers and a plurality of encryption key identifiers, to an authenticating device, the plurality of algorithm identifiers and the plurality of encryption key identifiers stored;
>
> a first receiving step to receive the plurality of algorithm identifiers and the plurality of encryption key identifiers transmitted from the authenticated device by the first transmitting step, at the authenticating device storing at least one algorithm identifier and at least one encryption key identifier;
>
> a selecting step to select, at the authenticating device, a prescribed algorithm identifier and a prescribed encryption key identifier to be stored by the authenticating device from among the plurality of algorithm identifiers and the plurality of encryption key identifiers received by the receiving step, when the at least one algorithm identifier and the at least one encryption key identifier stored by the authenticating device exist among the plurality of algorithm identifiers and the plurality of encryption key identifiers received by the first receiving step;
>
> a second transmitting step to transmit the prescribed algorithm identifier and the prescribed encryption key identifier selected by the selecting step, from the authenticating device to the authenticated device;
>
> a second receiving step to receive the prescribed algorithm identifier and the prescribed encryption key identifier transmitted by the second transmitting step, from the authenticating device, at the authenticated device.

Appellants respectfully submit that the Examiner's reasoning provided in support of the rejection of independent claim 7 under 35 U.S.C. § 102(e) as being anticipated by Edgett fails to establish *prima facie* anticipation. The deficiencies of the rejection are at least in that Edgett fails to disclose the above-noted features of independent claim 7.

In response to the Appellants' arguments regarding claim 7, the Examiner responds with new arguments on the interpretation of the teachings of Edgett. Specifically, the Examiner asserts in the Examiner's Answer on pages 17 to 19 as follows:

> ... Edgett does teach transmitting and receiving a plurality of algorithm identifiers stored between an authenticating device and an authenticated device...[t]he algorithm identifiers in this case are one of many that are transmitted back and forth between the network user (authenticated device) and the Server (decryption/update servers) (authenticating device) as there is both an old algorithm and a new algorithm (plurality of algorithms) and they can overlap until the user is migrated (paragraphs 0058-0059). Therefore the algorithm identifier serves the purpose of identifying which algorithm, old or new, is supposed to be used in the encryption/decryption process to be carried out between the user and the Servers.
>
> ... Edgett does teach transmitting and receiving a plurality of encryption key identifiers stored between an authenticating device and an authenticated device...Edgett discloses that there is a plurality of overlapping key pairs which may each be defined by a key index (key identifier) (paragraph 0053). Therefore, the key index allows the decryption server to select which one of the overlapping key pairs is to be used in the encryption/decryption process (paragraph).

In view of the above arguments, the Examiner is mischaracterizing Edgett in an effort to satisfy the claimed features. Contrary to the assertion by the Examiner, Edgett does not teach or suggest **transmitting or receiving** a plurality of algorithm identifiers and a plurality of encryption key identifiers stored between an authenticating device and an authenticated device as claimed. According to the Examiner's arguments, the old algorithm identifier and the new algorithm identifier overlapped correspond to the claimed plurality of algorithm identifiers and the old key index and the new key index overlapped correspond to the claimed plurality of

encryption key identifiers. However, even assuming, *arguendo*, the Examiner's assertion is true, Edgett still does not disclose or suggest **transmitting or receiving** the old algorithm identifier and the new algorithm identifier together, or **transmitting or receiving** the old key index and the new key index together. To the contrary, Edgett discloses that the user transmits and the decryption/Update servers receive old (single) algorithm identifier and old (single) key index during an authentication process, or that the decryption/Update server transmits and the user receives new (single) algorithm identifier and new (single) key index during an updating process. Nowhere in Edgett is there a disclosure or suggestion of transmitting or receiving a plurality of algorithm identifiers and a plurality of encryption key identifiers between an authenticated device and an authenticating device as claimed.

As such, Appellants maintain that the Examiner has failed to establish *prima facie* anticipation in the rejection of claim 7.

D. The Rejection Fails to Establish *Prima Facie* Anticipation of Independent Claim 8

The Examiner does not provide additional arguments with respect to claim 8. Appellants maintain that, as argued above and in Appellants' Appeal Brief, Edgett fails to teach or suggest all of the claim elements.

As such, Appellants maintain that the Examiner has failed to establish *prima facie* anticipation in the rejection of claim 8.

E. The Rejection Fails to Establish *Prima Facie* Anticipation of Independent Claim 9

The Examiner does not provide additional arguments with respect to claim 9. Appellants maintain that, as argued above and in Appellants' Appeal Brief, Edgett fails to teach or suggest all of the claim elements.

As such, Appellants maintain that the Examiner has failed to establish *prima facie* anticipation in the rejection of claim 9.

F. The Rejection Fails to Establish *Prima Facie* Anticipation of Independent Claim 10

The Examiner does not provide additional arguments with respect to claim 10. Appellants maintain that, as argued above and in Appellants' Appeal Brief, Edgett fails to teach or suggest all of the claim elements.

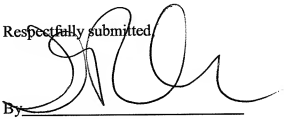
As such, Appellants maintain that the Examiner has failed to establish *prima facie* anticipation in the rejection of claim 10.

IV. CONCLUSION

For all the reasons set forth above, the rejections in the Examiner's Answer dated January 26, 2010, are improper. It is therefore respectfully requested that the Examiner be reversed on all grounds.

Dated: March 24, 2010

Respectfully submitted,



By _____
D. Richard Anderson
Registration No.: 40,439
BIRCH, STEWART, KOLASCH & BIRCH, LLP
8110 Gatehouse Road
Suite 100 East
P.O. Box 747
Falls Church, Virginia 22040-0747
(703) 205-8000
Attorney for Applicant